NHS

Walsall Clinical Commissioning Group

Information Security & Access Control Policy

Information Security & Access Control Policy

For

Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 05 March 2019
Signed: Chair of the committee
Signed: Designated Senior Officer

2.0

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	**V3.0**
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	05 March 2019
Date Policy is Effective From	Ratification date
Expiry date:	March 2020
Review date:	January 2020
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	CCG staff
National Documents	General Data Protection Regulation Network & Information Systems Regulations 2017 Anti-Virus & Malware Guidelines NHS Digital Standards
CCG linked documents	IM&T policy RA Policy Disciplinary Policy Raising Concerns at Work (Whistleblowing) Policy Acceptable Use Guidelines Computer Misuse Act 1990
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	BCC FOI Policy v 0.4

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation
Nigel Malone	Infrastructure Service Manager
Vicki Cooper	IT Service Delivery Manager
Mark Taylor	Assistant Director IT Services

2.0

Richard Corbett	Infrastructure Support Manager
Sharon Thomas	Corporate Governance Manager

Circulated to the following for consultation

Name/Committee/Group/	Designation
Director of Strategy & Improvement & SIRO	Walsall Healthcare NHS Trust
IG Function Leads	
Audit and Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments

Version Control Summary

Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author
0.1	13/11/17	Initial draft	Maz Healey
1.2	09/05/18	Updated draft	Maz Healey
1.3	20/6/18	Updated draft	Maz Healey
2.0	01/02/19	Complete review following introduction of GDPR and best practice exercise	Sharon Thomas
2.1	25/09/19	Reference to Walsall Clinical Commissioning Group	Serena Ellis

Contents

INFORMATION SECURITY & ACCESS CONTROL POLICY

1.0 Introduction

The Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of the organisation's information. It is the overarching policy for information security and supported by specific technical security, operational security and security management procedures.

2.0 Purpose of Policy

The purpose of this Information Security and Access Control Policy and its associated documents is to ensure the CCG has an overall digital information security management framework; to protect, to a consistently high standard, all CCG digital information assets, including patient records and other NHS corporate information from all potentially damaging threats, whether internal or external, deliberate or accidental.

All users of CCG IT systems must abide by the rules set out in this document. Users will be held personally responsible for failure to comply with the policy and may be subject to disciplinary action.

3.0 Statement of Intent

The CCG is obliged to abide by all relevant UK and European Union legislation. The requirements to comply with this legislation shall be devolved to employees and agents of the CCG, who may be held personally accountable for any breaches of information security; failure to comply could result in the individual or the CCG being prosecuted. The CCG shall comply with the legislation, detailed in this document, and other legislation as appropriate.

4.0 Scope and limitations

This policy applies to all areas and activities of the CCG, including system accounts, and to all individual users employed by the CCG including contractors, volunteers, students, locum and agency staff, staff employed on honorary contracts, and any other individual or organisation granted access to CCG systems. This policy applies to all information held on electronic assets.

4.1 OBJECTIVES

The objectives of this policy are to preserve:
Confidentiality – access to data is confined to those who have legitimate authority to view it.
Integrity – data is timely and accurate and detected or amended only by those specifically authorised to do so.
Availability – information shall be available and delivered to the right person, at the time when it is needed.

5.0 ROLES AND RESPONSIBILTIES

5.1 Members of the Information Governance Operational Group

The operational Information Governance lead is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating Information Governance in the CCG and raising awareness of Information Governance.

Through this group, the Audit and Governance committee are advised of common approaches to information governance/security and assured of CCG practices

5.2 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

The aim of the Caldicott Guardian is to ensure the organisation implements the Caldicott principles and data security standards.

5.3 1.0 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is accountable for information risk within the CCG and advises the Governing Body on the effectiveness of information risk management across the organisation.

5.4 Information Asset Owners/Local Record or Senior Managers

The aim of the IAO role is to have a nominated role or person to be responsible for the management and control of information assets.

The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and shall be responsible for:

(i) Understanding what information is held.
(ii) Knowing what is added and what is removed.
(iii) Understanding how information is moved.
(iv) Knowing who has access and why.

5.5 All Staff (with individual responsibilities under the policy)

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting CCG business. All staff members are responsible for information security and remain accountable for their actions in relation to NHS and other UK Government information and information systems. Staff shall ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

5.6 Data Protection Officer

The Data Protection Officer is responsible for ensuring that the CCG and its constituent business areas remain compliant at all times with Data Protection, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer shall:

(i) Lead on the provision of expert advice to the organisation on all matters concerning the Data Protection Act, compliance, best practice and setting and maintaining standards.

(ii) Provide a central point of contact for the Act both internally and with external stakeholders (including the Office of the Information Commissioner).

(iii) Communicate and promote awareness of the Act across the organisation.

(iv) Lead on matters concerning individual's right to access information held by the CCG and the transparency agenda.

6.0 PROCEDURE

This policy sets out the high level framework for Information Security within the CCG.

In conjunction with information governance and data security principles, the aim of this policy is to establish and maintain the security and confidentiality of information within digital information systems, applications and networks owned or held by the CCG, by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and associated policies and procedures, through auditing, monitoring and reporting.

- Introducing a consistent approach to information security, ensuring that all members of staff fully understand their own responsibilities.

- Describing the principles of information security and explaining how they shall be implemented in the CCG.

- Creating and maintaining within the CCG a level of awareness of the need for information security as an integral part of the day to day business.

- Protecting information assets under the control of the CCG, to include any hosted or external applications.

- Ensuring staff do not remove information from the CCG unless approved to do so in consultation with Information Governance.

6.1 Information Security Awareness & Training

Information security awareness is included in the mandatory training programme. An ongoing awareness programme is in place and maintained to ensure that staff awareness is refreshed and updated as necessary through the Information Governance annual mandatory training programme.

6.2 Contracts of Employment

Staff security requirements are addressed at the recruitment stage and all contracts of employment will contain a confidentiality clause. Information security expectations of staff are including within appropriate job definitions.

6.3 Security Control of Assets

Each IT asset, (hardware, software, application or data; internally or externally supplied) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset. IAOs can be assisted by one or more Information Asset Administrators (IAA). Information Governance maintains a copy of the asset register.

The flow of data between an IAO's assets and any internal or external systems or parties

shall be included in the asset register.

Agreements with suppliers shall include requirements to address information security risks.

6.4 Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted services, or areas containing information systems or stored data. Exceptional access privileges will only be given with approval from the Senior Information Risk Owner (SIRO).

6.5 User Access Controls

Access to information shall be restricted to authorised users who have a legitimate business need to access the information and in accordance with the principle of least privilege.

6.6 Computer Access Controls

Access to computer facilities shall be restricted to authorised users who have a business need to use the facilities.

6.7 Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a licence from the supplier.

6.8 Digital Equipment Security

In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. This will be achieved by the effective use of suitable security measures i.e. physical controls within buildings, entry systems and secure storage facilities to protect assets from theft/damage.

6.9 Computer and Network

Management of computers shall be controlled through standard documented procedures that have been authorised by the CCG.

IT schedules back-ups on business critical databases and network files to enable recovery. Off-line, network disconnected copies shall be kept in addition to network accessible copies.

CCG digital equipment must not be used for private work, commercial activities, advertising or fundraising if not directly connected with the CCG unless it has had formal CCG approval.

Network integrity shall be protected through employing segregation and cryptographic

techniques where appropriate.

6.10 Remote Access

Remote access to CCG network and systems shall be through software and services provided by the CCG which requires additional user authentication. Staff and third party suppliers using remote access facilities shall do so from private locations and using secure network connections.

Third party support access will be provided by IT Services, via accounts providing the least privilege necessary to perform the required duties for the shortest amount of time.

Staff shall ensure that computers used for remote access are using up to date malicious software ('malware') protection. Any personally identifiable data (PID) or CCG intellectual property accessed from remote locations shall not be stored locally.

Staff will ensure that family and friends do not have access to CCG services and systems at the remote location and protect against eaves-dropping when using mobile devices in public places.

6.11 Information Risk Assessment

The principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis by their IAO in line with Risk Management Strategy and Policy. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

The NHS Digital good practice guides, National Cyber Security Centre (NCSC) 10 steps to Cyber Security, NCSC Cyber Essentials assurance framework and ISO 27001 Information Security Management Standard will be considered when risk assessing information security risks.

6.12 Information Security Events and Weaknesses

All information security events and suspected weaknesses are to be reported to the IT Service Desk. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events. Incidents and near misses will be reported in line with the CCG's Reporting and Management of Incidents, including serious incidents, policy. External event reporting will be in agreement between Information Governance and Information Technology departments.

The primary goal of handling an information security incident shall be to resume the

normal security level, followed by the necessary recovery and corrective actions. Information security threat and vulnerability information is to be received and actively sought from a variety of authoritative and special interest information sharing sources.

Serious events that require forensic investigation will do so in accordance with the NHS Digital Forensic Readiness Good Practice Guide.

Reporting must happen as soon as the event is discovered.

Software and hardware shall be maintained through its lifetime with the implementation of updates and alternatives ('patches').

6.13 Protection from Malware

The CCG shall use software countermeasures and management procedures to protect itself against the threat of malware. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the CCG property without permission from the CCG; any such requirements must be raised with the IT Service Desk, by logging a call. Users breaching this requirement may be subject to disciplinary action. The CCG shall undertake scans for vulnerabilities from malware.

6.14 User Media

Removable media of all types that contain software or data from external sources, or that have been used on external digital equipment, require the approval of the CCG before they may be used on CCG systems. Read only access to removable media is permitted, provided such media is fully virus checked before being used on the CCG equipment. Users breaching this requirement may be subject to disciplinary action.

6.15 Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on a regular basis; in so far as is practically possible, subject to technical limitations. The scope and retention of audit trail data shall be sufficient to support retrospective analysis of individuals' activities.

The CCG has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right to monitor activity where it suspects that there has been a breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- establishing the existence of facts;
- investigating or detecting unauthorised use of the system;
- preventing or detecting crime;
- ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training);
- in the interests of national security;
- ascertaining compliance with regulatory or self-regulatory practices or procedures.
- ensuring the effective operation of the system

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act.

6.16 Accreditation of Information systems

The CCG shall ensure that all new information systems, applications and networks include an approved security plan before they commence operation.

IAOs are responsible for carrying out Impact Assessments, annual risk assessments/reviews for systems under their control.

6.17 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CCG. IT changes are subject to the completion and approval of the 'Request for Change' form. System developments shall follow a defined life cycle.

6.18 Intellectual Property Rights

The CCG shall ensure that all digital information products are properly licenced and approved by the CCG. The CCG will take appropriate steps to protect its intellectual property rights to any locally developed systems and will protect that right accordingly.

6.19 Business Continuity & Disaster Recovery Plans

The CCG shall ensure that business impact assessments, business continuity and disaster recovery plans are produced, tested and deployed when necessary for all mission critical digital information, applications, systems and networks.

6.20 Digital Equipment Disposal

NHS and third party systems which deal with personal identifiable data (PID), confidential or sensitive information will be disposed of in line with national requirements to prevent unauthorised disclosure.

All redundant equipment must be disposed of in line with:

- NHS Digital disposal and Destruction of Sensitive Data
- The Information Commissioner's Office (ICO) IT asset disposal for organisations
- The Waste Electronic and Electrical Equipment Directive (WEEE)

7.0 EQUALITY IMPACT ASSESSMENT

The users of this policy will take into account their statutory duty to promote equality and human rights and to act lawfully within current equality legislation and guidance.

This policy has been equality impact assessed and has been shown to have no adverse impact on any equality group.

The CCG will continue to monitor its effect and will assess again if negative impact is identified or at the review date.

7.1 Financial implications

Any financial implications will be considered as part of the annual budget setting process across the CCG

7.2 Risk Implications / Risk Assessment

There are no risk implications associated with this policy subject to successful implementation and compliance. The implementation of this policy mitigates risk around inappropriate use of digital assets and the standards within Data Security and Protection Toolkit.

8.0 MONITORING, CONTROL AND AUDIT

Monitoring Process	**Requirements**
Who	The Threat Assessment Group (TAG)
Standards Monitored	• Audit of system access and data use by staff; • Trend analysis on system access; • Review of enhanced privileged access assignment to digital information assets; • Reports on lost or stolen mobile devices; • Reports on redundant mobile devices usage; • Monitoring of network activity.
When	Bi-annually
How	Audit
Presented to	Information Governance Operational Group
Monitored by	Information Governance Operational Group
Completion/Exception reported to	Audit & Governance Committee
Who	Information Governance Manager
Standards Monitored	Completion of mandatory data security and awareness training
When	Bi-annually
How	Audit
Presented to	Information Governance Operational Group
Monitored by	Information Governance Operational Group
Completion/Exception reported to	Audit & Governance

Areas of non-conformance will be highlighted to the relevant departments and recommendations suggested to tighten controls or make adjustments to related procedures.

9.0 TRAINING

Information security awareness is included in the mandatory training. Ongoing information awareness take place throughout the year to ensure that staff awareness is maintained.

Training is provided both face to face and via e-learning and this includes specific training for Information Asset Owners/Administrators.

10.0 DEFINITIONS

The following terms are used within this policy:

AV	Anti-virus
GDPR	General Data Protection Regulations
IAA	Information Asset Administrator
IAO	Information Asset Owner
IGSG	Information Governance Steering Group
IT	Information Technology
RMC	Risk Management Committee
SIRO	Senior Information Risk Owner
TAG	Threat Assessment Group. It consists of 4 members of IT Services: IT Business Manager, Infrastructure Services Manager, Infrastructure Support Manager, Server SME all of whom are based at Eldon Court.

11.0 BEST PRACTICE, EVIDENCE AND REFERENCES

- Freedom of Information Act 2000
- Health & Social Care (Safety & Quality) Act 2015
- Computer Misuse Act 1990
- Network and Information System Regulations (NIS) 2017
- The General Data Protection Regulations/ Data Protection Act 2018
- Human Rights Act 1998
- Information Security Management: NHS Code of Practice – DH 2007
- Information Security Code of Practice – DH
- NHS Digital Information Governance Toolkit
- Telecommunications (Lawful Business Practice) Interception of communications regulations 2000
- Risk Management Strategy & Policy/Procedures
- Information Governance Policy